1 of 3

#20 3/31/04 DS

Docket No.: 64965-054 **PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| In re Application of | : | Customer Number: 20277 |
| Shashank MERCHANT, et al. | : | Confirmation Number: 7187 |
| Serial No.: 09/315,973 | : | Group Art Unit: 2667 |
| Filed: May 21, 1999 | : | Examiner: Anh Vu H Ly |

For: NETWORK SWITCH WITH MULTIPLE-PORT SNIFFING



## APPEAL BRIEF

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed February 2, 2004.

## I. REAL PARTY IN INTEREST

The real party in interest is Advanced Micro Devices, Inc, the assignee of the entire right, title and interest in and to the above-identified U. S. Application.

## II. RELATED APPEALS AND INTERFERENCES

No other appeals or interferences are known to the Appellant which will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal.

## III. STATUS OF CLAIMS

Claims 1-19 are pending. Claims 7-13 and 19 are found allowable subject to being

rewritten in independent form. Claims 1-6 and 14-18 stand under final rejection, from which rejection this appeal is taken.

## IV. STATUS OF AMENDMENTS

The Application has not been amended after the final Office Action.

## V. SUMMARY OF INVENTION

The present invention relates to a multiport network switch having a sniffing system that enables a sniffer or network-analyzing probe connected to a sniffer port to monitor receive and transmit traffic on multiple other ports of the switch.

As shown in Figure 2 of the application, a multiport switch 12 contains a decision making engine or an internal rules checker (IRC) 40 that performs frame forwarding decisions, and a switching subsystem 42 for transferring frame data according to the frame forwarding decisions. The IRC 40 monitors the data bus to determine the frame pointer value and the header information of the received packet (including source, destination, and VLAN address information). The IRC 40 uses the header information to determine which MAC ports will output the data frame stored at the location specified by the frame pointer. The IRC 40 may thus determine that a given data frame should be output by either a single port, multiple ports, all ports (i.e., broadcast) or no ports (i.e., discarded).

As shown in Figure 4, the IRC 40 may contain multiple rules queues 102 arranged for holding frame pointers and frame header information. A single rules queue 102 is assigned to each receive port of the switch 12 for storing information associated with the frames received via the corresponding port. In particular, rules queues 1 to 12 may be provided for 10/100 MAC ports 1 to 12 configured to receive data from the corresponding 10/100 Mb/s network stations 14, a rules queue 13 may be arranged to support the gigabit MAC port 24 capable of receiving data

from the gigabit network node 22, and a rules queue 14 may be assigned to the expansion port 30.

Frame headers and frame pointers from the rules queues 102 are transferred to IRC logic circuits such as ingress rules logic 106, source address (SA) lookup logic 108, destination address (DA) lookup logic 110 and egress rules logic 112 to produce a forwarding descriptor supplied to the port vector FIFO 56. The IRC scheduler 104 provides time slots for sequential transferring data held in the rules queues 102 to the IRC logic circuitry.

The egress logic circuit 112 checks each transmit port in the port vector produced by the DA lookup logic circuit 110 to remove or mask the disabled ports, the ports that do not belong to a required VLAN, and the port from which the frame is received. Also, the egress logic circuit 112 performs a sniffing function to monitor data traffic on selected ports. As a result, the egress rules logic circuit 112 generates a forwarding descriptor including a port vector field identifying each MAC port that should receive the corresponding frame, a receive port field indicating the port from which the frame was received, and an operation code field containing instructions about how the frame should be modified before transmission. Also, the forwarding descriptor may contain fields indicating priority queues, VLAN identifiers, the location of the frame in the external memory, etc.

The egress rules logic 112 provides a sniffer port traffic capture mechanism, which allows a network analyzing probe connected to a port designated as the sniffer port to monitor or sniff network activity on multiple ports designated as the sniffed ports. As shown in Figure 5, the sniffer port traffic capture mechanism comprises a sniffer port configuration (SNIFR) register 120 and a sniffed port configuration (SNIFD) register 122. The SNIFR register 120 configures a sniffer port to receive all receive and transmit traffic from a set of sniffed ports. For example, as

shown in Figure 5, the port 2 may be configured as the sniffer port, and ports 4 and 6 may be designated as the sniffed ports. The SNIFR register 120 contains a 4-bit sniffer port field identifying the sniffer port.

In addition, the SNIFR register 120 contains a sniff enable bit, which enables or disables the sniffer function. When the sniff enable bit is set, the sniffer port traffic capture mechanism is enabled. When the sniff enable bit is reset, the sniffer port traffic capture mechanism is disabled. The SNIFD register 122 contains a 14-bit sniffed port vector that configures a set of sniffed ports. Each bit of the sniffed port vector corresponds to one of the fourteen ports of the IMS 12. To designate a set of ports as the sniffed ports, the corresponding bits of the sniffed port vector may be set. Thus, multiple ports of the IMS 12 may be configured as sniffed ports. When the sniff enable bit and one or several bits of the sniffed port vector are set, data received and transmitted by the corresponding sniffed ports are also transferred to the sniffer port indicated in the SNIFR register 120.

When the sniff enable bit is set, the egress rules logic circuit 112 producing a forwarding descriptor inspects the receive port number and the port vector for each frame. If the receive port number or any of the ports identified in the port vector supplied to the egress logic circuit 112 corresponds to one of the sniffed ports programmed in the SNIFD register 122, the egress logic circuit 112 adds the sniffer port programmed in the SNIFR register 120 to the port vector field of the forwarding descriptor. Then, the egress logic circuit 112 transfers the produced forwarding descriptor to the port vector FIFO 56. The port vector field is examined by the port vector FIFO 56 to determine which particular output queues correspond to the sniffer port and other ports selected for transmission, and should receive the associated frame pointer. The port vector FIFO 56 places the frame pointer into the top of the corresponding queues. Thus, data frames received

or transmitted by sniffed ports will be copied to the sniffer port. As a result, a network-analyzing probe connected to the sniffer port is enabled to monitor all data frames received or transmitted by any of sniffed ports.

## VI. ISSUES

Whether claims 1-6, and 14-18 are unpatentable over Gridley (6,522,656) in view of Murthy et al. (5,515,376) under 35 U.S.C. § 103.

## VII. GROUPING OF CLAIMS

Appellant submits that the claims of the rejected group do not stand or fall together, the claims being considered to be separately patentable for the reasons presented in the Argument section of this Brief.

## VIII. THE ARGUMENT

In the application of a rejection under 35 U.S.C. §103, it is incumbent upon the Examiner to factually support a conclusion of obviousness. As stated in ***Graham v. John Deere Co.*** 383 U.S. 1, 13, 148 U.S.P.Q. 459, 465 (1966), obviousness under 35 U.S.C. §103 must be determined by considering (1) the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims in issue; and (3) resolving the level of ordinary skill in the pertinent art. The Examiner must provide a reason why one having ordinary skill in the art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. ***Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.***, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985). ***In re Fine***, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); ***Stratoflex, Inc. v. Aeroquip Corp.***, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); ***In re Warner***, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967).

These showings by the Examiner are an essential part of complying with the burden of

presenting a *prima facie* case of obviousness. ***In re Oetiker***, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).

As demonstrated below, the Examiner has failed to provide proper reasons for modifying the prior art and thus to establish a *prima facie* case of obviousness.

Independent claim 1 recites a multiport data communication system for transferring data packets between ports. The data communication system comprises a plurality of ports for receiving and transmitting the data packets, and a decision making engine responsive to received data packets for directing the received data packets to the ports selected for transmission of the received data packets.

The decision making engine includes:

- a plurality of queuing devices corresponding to the plurality of ports for queuing data blocks representing the data packets received by the corresponding ports,

- logic circuitry responsive to the plurality of queuing devices for processing the data blocks in accordance with a prescribed algorithm to determine destination information,

- a forwarding circuit responsive to the logic circuitry for identifying at least one transmit port , and

- a traffic capture mechanism for enabling one port of said plurality of ports to output data transferred via multiple other selected ports of said plurality of ports.

The Examiner holds Gridley to differ from the claimed subject matter only in that the reference does not disclose the claimed traffic capture mechanism. Murthy et al. is relied upon for disclosing this element.

The Examiner takes the position that "since Gridley mentions about monitoring operation within the switch but does not disclose a traffic capture mechanism for enabling one port to

output data transferred via selected ports," it would have been obvious to include this feature "to monitor data packets and collect related information for network analysis." It is noted that the Examiner considers operations of the system controller of Gridley to be a monitoring operation that provides motivation for including the traffic capture mechanism in the Gridley system.

The Examiner's position of obviousness is respectfully traversed.

Gridley discloses a system controller 230 which monitors operation of each one of LAN cards 100A-100D, monitors the health of the Ethernet switch in genera,l such as crashing or improper operation of any one of the LAN cards, and keeps system statistics. Hence, the reference does not suggest that the system controller monitors traffic via ports of the LAN cards. Accordingly, no reason is apparent to support the conclusion that one having ordinary skill in the art would have been impelled to include into the system controller 230 a traffic capture mechanism for enabling one port of the LAN card to output data transferred via multiple other selected ports.

Moreover, Gridley does not disclose that the system controller 230 performs network analysis. Therefore, no reason exists to include the traffic capture mechanism "to monitor data packets and collect related information for network analysis," as the Examiner suggests.

The Examiner has apparently failed to give adequate consideration to the particular problems and solution addressed by the claimed invention. ***Northern Telecom, Inc. v. Datapoint Corp.***, 908 F.2d 931, 15 USPQ2d 1321 (Fed. Cir. 1990); ***In re Rothermel***, 276 F.2d 393, 125 USPQ 328 (CCPA 1960). The present invention provides a sniffing system that enables a sniffer or network-analyzing probe connected to a sniffer port of a switch to monitor traffic on multiple other ports of the switch.

Gridley does not recognize the problem of sniffing traffic on ports. Therefore, the

reference provides no reason for modification suggested by the Examiner.

Hence, the lack of any motivation for the proposed modification of Gridley to arrive at the claimed invention, coupled with the particular problems addressed and solved by the claimed invention, undermine the basis for the Examiner's rejection under 35 U.S.C. § 103.

Further, even if the references were combined, the claimed invention would not result. The Examiner has failed to ascertain the differences between the prior art and the claims in issue.

Considering the references, Gridley discloses a distributed processing system with multiprocessing configuration. The Examiner considers:

- the packet RAM 135 of Gridley to correspond to the plurality of queuing devices corresponding to the plurality of ports for queuing data blocks representing the data packets received by the corresponding ports; and

- the address processor 220 to correspond to the logic circuitry responsive to the plurality of queuing devices for processing the data blocks in accordance with a prescribed algorithm to determine destination information.

Considering the references, Gridley discloses that the packet RAM 135 serves as a packet buffer which stores the packets received through ports P1-P8 of the respective LAN while the packet processor sends the packet header of the packet stored in the packet RAM 135 to the system card (col. 3, lines 51-60).

The reference does not disclose that the packet RAM 135 serves as the plurality of queuing devices corresponding to the plurality of ports for queuing data blocks representing the data packets received by the corresponding ports of the plurality of ports for receiving and transmitting the data packets, as claim 1 requires.

The Examiner appears to admit this fact, because she takes the position that the "plurality

of queuing devices corresponding to the plurality of ports for queuing data blocks" is inherent to Gridley.

The Examiner's position is respectfully traversed for the following reasons.

It is well settled that inherency requires certainty, not speculation. ***In re Rijckaert***, 9 F.3rd 1531, 28 USPQ2d 1955 (Fed. Cir. 1993); ***In re King***, 801 F.2d 1324, 231 USPQ 136 (Fed. Cir. 1986); ***W. L. Gore & Associates, Inc. v. Garlock, Inc.***, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983); ***In re Oelrich***, 666 F.2d 578, 212 USPQ 323 (CCPA 1981); ***In re Wilding***, 535 F.2d 631, 190 USPQ 59 (CCPA 1976). To establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probability or possibilities. ***In re Robertson***, 169 F.3d 743, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

The Examiner contends that the packet RAM 135 is a shared packet memory having dynamically allocated portions for storing the received data packets corresponding to the claimed queuing devices.

However, the reference does not suggest that the received packets are stored in portions allocated for each port. For example, the same portion of the RAM 135 may store data received from several ports. Also, data received from one port may be distributed in various portions of the RAM 135. Therefore, the packet RAM 135 does not necessarily contain a plurality of queuing devices corresponding to the plurality of ports for queuing data blocks representing the data packets received by the corresponding ports. Hence, the Examiner's conclusion of inherency is not warranted.

Moreover, as indicated above, the address processor 220 of Gridley is considered to

correspond to the claimed logic circuitry responsive to the plurality of queuing devices for processing the data blocks in accordance with a prescribed algorithm to determine destination information.

Gridley discloses that the address processor 220 is responsive to packet source and destination information from multiple LANs to update and access the address RAM 225 which contains an address look-up table (col. 4, lines 3-6). Accordingly, the address processor 220 is not responsive to the plurality of queuing devices for processing the data blocks placed in data queues in accordance with a prescribed algorithm to determine destination information, as claim 1 requires.

Further, the Examiner asserts that "if the switch does not receive any data packets, store the data packets, then the functions such as forwarding decisions should not be happened [sic] at all."

It is noted that claim 1 specifically requires the logic circuitry **to be responsive to the plurality of queuing devices for processing the data blocks** (representing the data packets received by the corresponding ports) in accordance with a prescribed algorithm to determine destination information. Gridley does not disclose these features.

It is noted that in the Advisory Action, the Examiner indicated that she already responded to this argument. However, nothing in the Office Action addresses the issue of logic circuitry responsive to the plurality of queuing devices for processing the data blocks representing the data packets received by the corresponding ports.

It is respectfully submitted that Gridley does not teach or suggest that the address processor 220 is responsive to the plurality of queuing devices for processing the data blocks in accordance with a prescribed algorithm to determine destination information, as the claim requires.

Hence, Gridley does not disclose:

- a plurality of queuing devices corresponding to the plurality of ports for queuing data blocks representing the data packets received by the corresponding ports, and

- logic circuitry responsive to the plurality of queuing devices for processing the data blocks in accordance with a prescribed algorithm to determine destination information, as claim 1 recites

As the Examiner admits, Murthy also does not disclose these features.

It is well settled that the test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art. ***Cable Electric Products, Inc. v. Genmark, Inc.***, 770 F.2d 1015, 226 USPQ 881 (Fed. Cir. 1985). In determining whether a case of *prima facie* obviousness exists, it is necessary to ascertain whether the prior art teachings appear to be sufficient to one of ordinary skill in the art to suggest making the claimed substitution or other modification. ***In re Lalu***, 747 F.2d 703, 705, 223 USPQ 1257, 1258 (Fed. Cir. 1984).

As neither Gridley nor Murthy discloses or suggests the claimed elements listed above, the combined teachings of the references are not sufficient to arrive at the claimed invention. Hence, the Examiner's conclusion of obviousness with respect to claim 1 is improper.

Independent claim 14 recites that in a communication network having a plurality of ports and a decision making engine for controlling data forwarding between the ports, a method of monitoring network activity comprises the steps of:

- placing data blocks representing received data packets in a plurality of data queues to be processed by the decision making engine,

- processing the data queues by logic circuitry in accordance with a prescribed algorithm to determine destination information,

- identifying at least one port for transmitting data packets based on the destination information,

- selecting multiple sniffed ports among the plurality of ports for monitoring the data packets transferred via the sniffed ports, and

- selecting a sniffer port among the plurality of ports to provide output of the data packets transferred via the sniffed ports.

The Examiner admits that Gridley does not disclose the steps of selecting multiple sniffed ports among the plurality of ports for monitoring the data packets transferred via the sniffed ports, and selecting a sniffer port among the plurality of ports to provide output of the data packets transferred via the sniffed ports. Murthy is relied upon for disclosing these steps.

However, as discussed above, there is no motivation for modifying Gridley to carry out the selection of multiple sniffed ports among the plurality of ports for monitoring the data packets transferred via the sniffed ports, and the selection of a sniffer port among the plurality of ports to provide output of the data packets transferred via the sniffed ports.

Moreover, none of the references teaches or suggests placing data blocks representing received data packets in a plurality of data queues to be processed by the decision making engine, and processing the data queues by logic circuitry in accordance with a prescribed algorithm to determine destination information, as claim 14 requires.

Hence, the prior art teachings are not sufficient to one of ordinary skill in the art to suggest the method recited in claim 14. Accordingly, the Examiner's conclusion of obviousness with respect to independent claim 14 is not warranted.

Regarding dependent claims 2-6, and 15-18, the Examiner takes the position that it would have been obvious to modify Gridley to include the claimed features.

However, as discussed above, Gridley provides no reasons for arranging:

- a sniffer port for connecting to a probe for monitoring data traffic, and multiple sniffed ports monitored by the probe via the sniffer port, as claims 2 and 3 recite;

- a sniffer port configuration circuit for selecting the sniffer port among said plurality of ports, as claim 4 recites;

- a sniffed port configuration circuit for selecting the multiple sniffed ports among said plurality of ports, as claim 5 recites; and

- the sniffer port configuration circuit configured to enable and disable monitoring of data traffic on the multiple sniffed ports, as claim 6 recites.

Further, the Examiner relies upon Gridley for disclosing the step of identifying at least one port for transmitting data packets recited in claim 14. However, Gridley does not teach or suggest that this step comprises:

- the step of determining whether a port that received a data packet is one of the multiple sniffed ports, as claim 15 dependent from claim 14 recites, or

- the step of determining whether the destination information indicates that at least one of the multiple sniffed ports is selected for transmitting a data packet, as claim 17 dependent from claim 14 recites.

Accordingly, the combination of references is not sufficient to suggest these steps.

Moreover, claim 16 dependent from claim 15 recites that the sniffer port is identified as at least one of the ports for transmitting the data packet, if the port that received the data packet is one of the multiple sniffed ports, and claim 18 dependent from claim 17 recites that the sniffer port is identified as a port for transmitting the data packet, if at least one of the multiple sniffed ports is selected for transmitting the data packet. The reference combination neither teaches nor

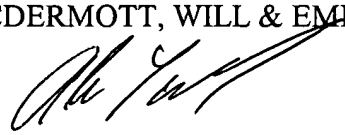
suggests these features.

## IX. CONCLUSION

For the reasons advanced above, Appellant respectfully contends that the rejection of claims 1-6, and 14-18 as being obvious under 35 U.S.C. § 103 is improper as the Examiner has not met the burden of establishing a *prima facie* case of obviousness. Reversal of the rejection in this appeal is respectfully requested

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Alexander V. Yampolsky
Registration No. 36,324

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 AVY:MWE
Facsimile: (202) 756-8087
**Date: March 25, 2004**

## X. APPENDIX

1. A multiport data communication system for transferring data packets between ports, the data communication system comprising:

a plurality of ports for receiving and transmitting the data packets,

a decision making engine responsive to received data packets for directing the received data packets to the ports selected for transmission of the received data packets,

the decision making engine including:

a plurality of queuing devices corresponding to the plurality of ports for queuing data blocks representing the data packets received by the corresponding ports,

logic circuitry responsive to the plurality of queuing devices for processing the data blocks in accordance with a prescribed algorithm to determine destination information,

a forwarding circuit responsive to the logic circuitry for identifying at least one transmit port , and

a traffic capture mechanism for enabling one port of said plurality of ports to output data transferred via multiple other selected ports of said plurality of ports.

2. The system of claim 1, wherein said one port is a sniffer port for connecting to a probe for monitoring data traffic.

3. The system of claim 2, wherein said multiple other selected ports are multiple sniffed ports monitored by the probe via the sniffer port.

4. The system of claim 3, wherein said traffic capture mechanism comprises a sniffer port

configuration circuit for selecting the sniffer port among said plurality of ports.

5. The system of claim 3, wherein said traffic capture mechanism comprises a sniffed port configuration circuit for selecting the multiple sniffed ports among said plurality of ports.

6. The system of claim 5, wherein said sniffer port configuration circuit is configured to enable and disable monitoring of data traffic on the multiple sniffed ports.

14. In a communication network having a plurality of ports and a decision making engine for controlling data forwarding between the ports, a method of monitoring network activity, comprising the steps of:

placing data blocks representing received data packets in a plurality of data queues to be processed by the decision making engine,

processing the data queues by logic circuitry in accordance with a prescribed algorithm to determine destination information,

identifying at least one port for transmitting data packets based on the destination information,

selecting multiple sniffed ports among the plurality of ports for monitoring the data packets transferred via the sniffed ports, and

selecting a sniffer port among the plurality of ports to provide output of the data packets transferred via the sniffed ports.

15. The method of claim 14, wherein the step of identifying at least one port for transmitting

data packets comprises determining whether a port that received a data packet is one of the multiple sniffed ports.

16. The method of claim 15, wherein the sniffer port is identified as at least one of the ports for transmitting the data packet, if the port that received the data packet is one of the multiple sniffed ports.

17. The method of claim 14, wherein the step of identifying ports for transmitting data packets comprises determining whether the destination information indicates that at least one of the multiple sniffed ports is selected for transmitting a data packet.

18. The method of claim 17, wherein the sniffer port is identified as a port for transmitting the data packet, if at least one of the multiple sniffed ports is selected for transmitting the data packet.